Clinical Communication Among Health Providers and Systems using Web Tools

James R. Flanagan, M.D., Ph.D. [a,b], Robert R. Montgomery [a]

[a]Division of Clinical Informatics, Information Systems Department, University of Iowa Hospitals and Clinics, and [b]Department of Internal Medicine, University of Iowa, Iowa City, Iowa

ABSTRACT

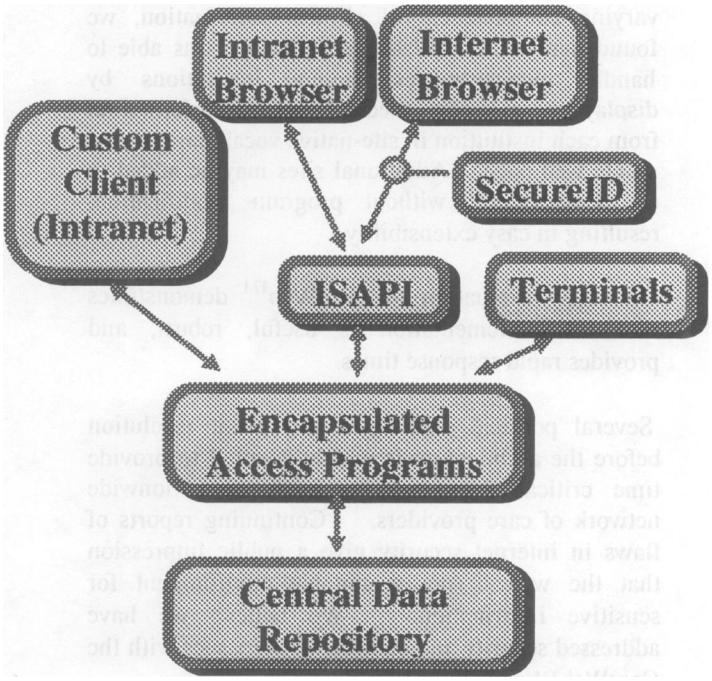
Three needs have driven the development of a Web front end to our legacy system. 1) A Web Intranet is needed to provide service for the quantity and diversity of platforms within our health care system. 2) Information transfer in our system is required in more than one format: in viewer-friendly, HTML format and in a database-friendly, down-loadable format. 3) The system encounters the need to electronically exchange information with providers that are not employees of our health care enterprise. This presents a problem with the authentication aspect of security for which we have devised a system to allow the carefully-monitored exchange of records with care providers who are "strangers" to our system.

INTRODUCTION

The University of Iowa Hospitals and Clinics (UIHC) enterprise includes a single 871 bed hospital with approximately 8000 staff as well as a number of small clinics located within a 100 mile radius. The enterprise is in the process of developing an integrated computer based patient record (CBPR). As its core information system the enterprise uses INFORMM, a highly-integrated financial, resource scheduling, and clinical system which resides on an IBM mainframe. Leveraging the mainframe system, are a number of graphical user interface (GUI) applications (both custom-client and Web-based) that use the mainframe as a clinical data repository [1].

The system architecture, shown in Figure 1, shows the central data repository (IBM mainframe parallel transaction processors) that supports a network of mainframe terminals, custom Windows-client applications on a restricted-access network, Web-browser clients on a restricted access network, and Web-browser clients using the Internet. Access from all terminals and clients uses the same user-authentication system (ID and password) with the exception of the Internet browser, which requires an additional component. The "SecureID" is a credit-card sized device from Security Dynamics that generates a changing code that is required for access via the Internet. Also shared by all terminals and clients is a system of user-specific patient population limitations. Of most importance, all users share a common data set in the form of the Central Data Repository (CDR).

Figure 1: INFORMM-Web System Architecture



The need for Web access to the central data repository arose from three sources. First, although we continue to have a need for custom-designed Windows client applications, even within our intranet there are far too many personal computers with different platforms and configurations to allow for maintaining the custom Windows client applications on all of them. The custom Windows applications are limited to special uses and are maintained on a controlled subset of devices. Support for browser access to clinical data is provided by INFORMM-Web as described below.

1091—8280/97/$5.00

Second, while most users access data to be viewed immediately, a large number of users require data transfers to their own personal or departmental systems for clinical, administrative, and research purposes. This need represents a burden in the form of custom programming efforts to link the central data repository to foreign systems. The download capabilities of the INFORMM-Web system, described below, are a step towards a standards-based approach to sharing data with foreign systems.

Third, although normal security requires that all users be precisely identified through authentication, electronic exchange of information is needed between those known to our system (authenticated users) and those who are "strangers" to the system (non-authenticated users). Even in this time of consolidation of health care systems, patients exhibit a tenacious desire to exercise the freedom to transfer care among systems. Although there is some discussion of the perils of using the Internet for clinical records [2,3] there is little to be found in the way of practical advice for dealing with the security problem effectively. We outline the tools and procedures being developed to provide convenient and prompt access to health information while preserving the security and confidentiality of the patient record. Finally, we propose methods for evaluating the adequacy of safeguards in dealing with system "strangers".

INFORMM-Web

Within the framework of the system architecture described in the introduction, this tool provides browser access to the CDR. The main security features and functionality provided by INFORMM-Web are outlined in Table 1.

Because of the system architecture, we are able to provide a single system of authenticating users regardless of their mode of access to the CDR. The only exception is for users that connect from outside of the intranet. In that case, another element of authentication is required in the form of a changing identification number that the user must transfer from a card-sized device known as a SecureID card.

Patient (or patient group) selection also uses a common security element regardless of mode of access. This has two faces: restrictive in that it prevents providers from accessing patients outside their permitted population, and permissive in that one or more "personal" lists of patients are maintained for the convenience of each provider.

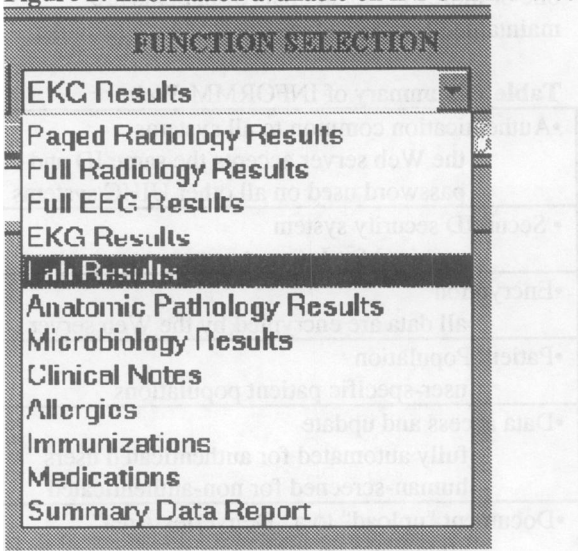
Table 1: Summary of INFORMM-Web

•Authentication common to all systems the Web server accepts the same ID and password used on all other UIHC systems
• SecureID security system required for Internet users
•Encryption all data are encrypted by the Web server
•Patient Population user-specific patient populations
•Data access and update fully automated for authenticated users human-screened for non-authenticated
•Document "upload" to a "Deliveries Area" allows system "strangers to send records to be reviewed by an authenticated user
•Knowledge links to Web knowledge resources convenient links to local and Internet Web resources such as the Virtual Hospital and the health sciences library are maintained.
•Information is available in two formats: HTML format for access with a Browser ASCII-delimited for import to databases (SGML-HL7 compatibility planned)
•Patient Data available in GUI includes: Laboratory, Micro., and Anatomic Path. Radiology, EKG, Holter, & EEG Reports 24 hr. summary of nursing notes and labs, Medications, Allergies, Immunizations, and Text Documents (Discharge Summ. etc.)
•All Other Patient Data in "Terminal Format": Using JAVA, the system provides browser support that includes a terminal emulator for access to data not yet available in GUI.

A key strategy that allows us to provide common access across the three interfaces is known in the industry as "encapsulation". Programs that access or update the CDR are encapsulated, separated from the programs that deal with the user interface.

On the other hand, not all information that is available on the mainframe interface has been made available through INFORMM-Web. The limitation, is not a large one. The range of functions available provides nearly all the information available in the CDR that is used by clinical providers. Figure 2 demonstrates information function selection.

Figure 2: Information available on INFORMM-Web



The INFORMM-Web interface requires the use of the frames technology available with certain Web browsers. A frame shows the selected patient. Others show available options, lists of results, and details of selected items from the lists. When a request for a knowledge link is made, the requested knowledge server (Virtual Hospital, Health Sciences Library, or other) is accessed within a frame on our site so that the context of the search can be maintained.

Information that is available on all interfaces, such as laboratory results, is displayed using the same conventions in all modes. For instance, Figure 3 demonstrates that abnormal laboratory results are marked as Abnormal, a sign indicates whether above or below the normal range, and the range is provided along with any abnormal result.

HUMAN & DATABASE FRIENDLY

The second need addressed in the introduction was for transfer of information in various formats. As shown in the Figure 4, authenticated users can select various ways to limit the information displayed or transferred. Data may be obtained on one patient or a pre-defined list of patients. The definition of the list of patients must be consistent with the population controls noted above or with special approval from the Institutional Review Board (IRB) for research involving human subjects. Information downloaded to other systems is subject to the same security requirements as information in

Figure 3: Results displayed.

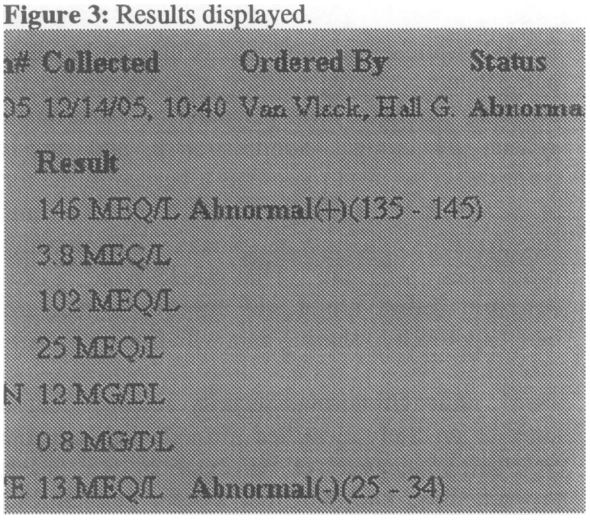
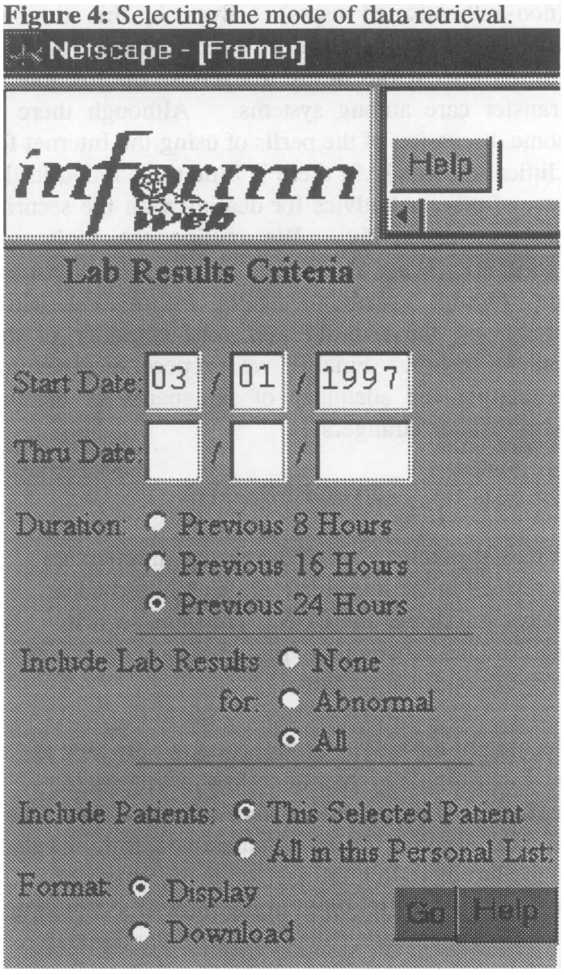


Figure 4: Selecting the mode of data retrieval.



the CDR and download users are audited to verify their compliance with security.

The most common format we use for data exchange is HL7 [4]. At this time we are not supporting other

formats, although we are following the development of the markup language intended for health care databases (SGML-HL7) with interest [5,6].

THE NON-AUTHENTICATED "STRANGER"

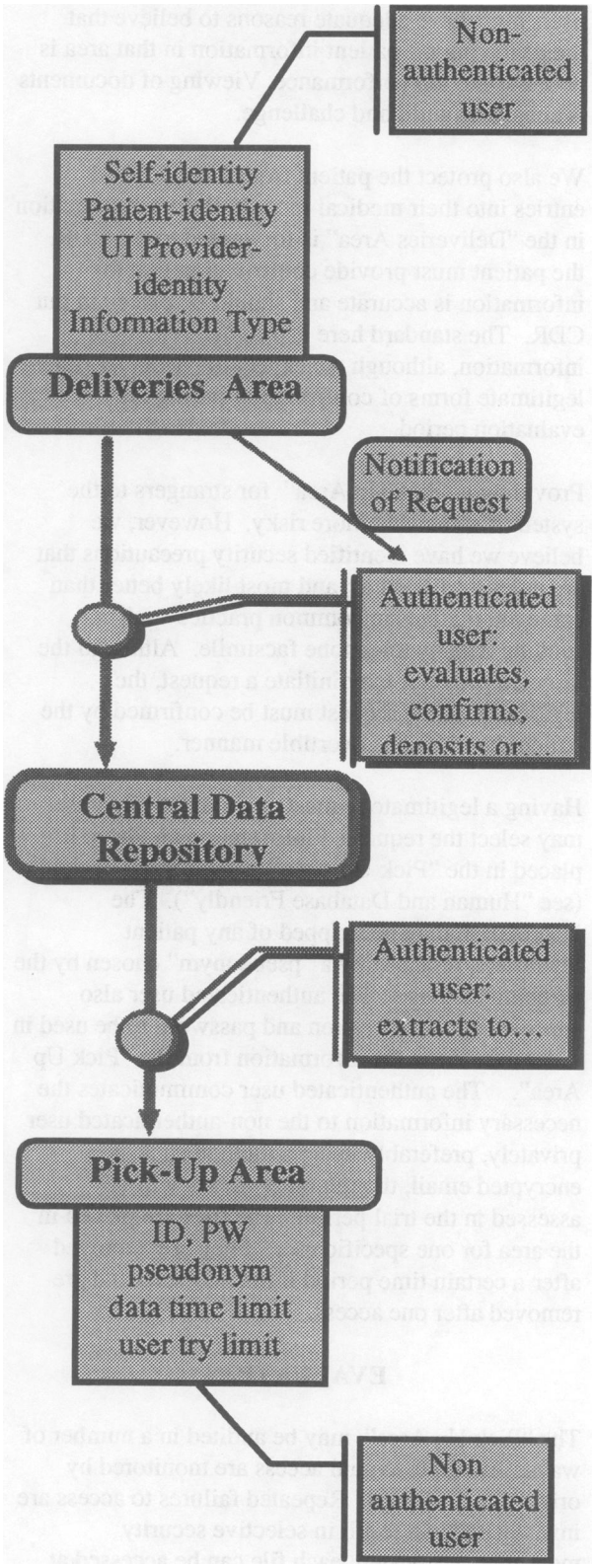
Any providers who have a legitimate and regular need to access information in the CDR are given the means to authenticate themselves and defined populations of patients they may access in the system. However, providers not known to the system may still have occasional legitimate needs to send or receive information. This brings us to the third need identified in the introduction.

For instance, a provider is sending a patient for a consultation and chooses to send us text and image documents using convenient Web tools. In another instance, a provider is accepting a patient in transfer and requests that we download text documents, images, and structured information (laboratory results) in a form that can be loaded into their system. Each of these providers has accompanied their requests with the image of a signed release from the patient. The patients have each communicated their wishes in writing to a UIHC authenticated provider.

Such situations occur repeatedly. It seems legitimate to respond to such needs as long as safeguards are adequate. Accordingly, we have designed the system described in Figure 5.

To understand this model, note that the security problem here is that the non-authenticated "stranger" to the system can not be positively identified with any certainty. Even if we can confirm that there is a legitimate provider by the name of the one given, such information is public and could be used by anyone. We propose such users place documents into a "Deliveries Area". This information is protected from viewing by non-authenticated users, including by the user who placed the information there. For non-authenticated users, it is a "Write Only" area. Each contribution to this area must be accompanied by the identifying information noted in Figure 5 with the exception of UI Provider identity, which may be unknown. The latter may be specified as a job position such as "Consulting Cardiologist" . The user must provide a statement to the effect that the patient has agreed that the information be communicated and, ideally, should provide an image of a release/consent form.

Figure 5: Dealing with System "Strangers"



Only an authenticated user of the system may view information in the "Deliveries Area". By policy, the users must have adequate reasons to believe that their viewing of patient information in that area is necessary to job performance. Viewing of documents is subject to audit and challenge.

We also protect the patient from unauthorized entries into their medical record. Before information in the "Deliveries Area" is forwarded to the CDR, the patient must provide confirmation that the information is accurate and should be placed in our CDR. The standard here is a signed release of information, although we expect to encounter other legitimate forms of confirmation during the evaluation period.

Providing a "Pick Up Area" for strangers to the system is somewhat more risky. However, we believe we have identified security precautions that are at least as good as, and most likely better than some alternatives in common practice such as sending data by telephone facsimile. Although the targeted provider may initiate a request, the legitimacy of the request must be confirmed by the patient in an incontrovertible manner.

Having a legitimate request, an authenticated user may select the requested information and have it placed in the "Pick Up Area" in the format desired (see "Human and Database Friendly"). The information may be stripped of any patient identifiers, replaced by a "pseudonym" chosen by the authenticated user. The authenticated user also specifies an identification and password to be used in order to retrieve the information from the "Pick Up Area". The authenticated user communicates the necessary information to the non-authenticated user privately, preferably using a method such as encrypted email, though other means will be assessed in the trial period. The files are placed in the area for one specific user. They are removed after a certain time period if not accessed and are removed after one access.

EVALUATION

The "Pick Up Area" may be audited in a number of ways. Attempts to gain access are monitored by origin of the request. Repeated failures to access are investigated and result in selective security measures. By design, each file can be accessed at most once. When the file is accessed, a message is sent to the intended receiver by alternate means. On a selective basis, the intended receivers are to be surveyed to determine whether the information was received. In these surveys we plan to monitor other aspects of the quality of the service such as its speed, accuracy of information delivered, and satisfaction of the provider and patient involved.

For information delivered to the system by non-authenticated users, similar factors may be audited. The source of files is monitored. Each delivery is to be assessed by the intended UI provider or by a Medical Records Technician for disposition. Delivery results in a message to the purported source of the information in order to detect inauthentic material. The assessment includes :

- is the patient is specified accurately / precisely
- is the UI provider is specified
- is the information is accurate (per patient)
- is the information is useful (per provider)
- does the delivery suggest attempted fraud.

Using these and other assessments, we will investigate whether we need to and how we may block undesired use of the system.

Ongoing evaluation will involve auditing the uses and handling of downloaded information by authenticated users. The ability to track the volume of downloaded information per user is a key benefit of providing the download service. In the present information environment users transfer information to their own personal devices, even if only on paper. Security is best served by giving providers satisfactory access to information in such a way that proper handling can be encouraged and monitored.

REFERENCES

[1] Flanagan, J.R., Chun, J., Wagner, J. Evolution of a Legacy System to a Web Patient Record Server: Leveraging Investment While Opening the System. pp. 618-622, JAMIA Symposium Supplement, AMIA Proceedings. 1996

[2] Doyle DJ. Surfing the Internet for patient information: the personal clinical web page [letter]. JAMA. 274(20):1586. 1995.

[3] Doyle DJ. Informal clinical consulting via the Internet [letter]. Canadian Medical Association Journal. 154(8):1150. 1996

[4] http://www.mcis.duke.edu/standards/HL7/hl7

[5] http://www.sil.org/sgml/gen-apps.html#HL7-SGML

[6] http://www.mcis.duke.edu/standards/HL7/sigs/sgml/